World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:10, No:10, 2016

Pre-Shared Key Distribution Algorithms' Attacks for Body Area Networks: A Survey

Authors : Priti Kumari, Tricha Anjali

Abstract : Body Area Networks (BANs) have emerged as the most promising technology for pervasive health care applications. Since they facilitate communication of very sensitive health data, information leakage in such networks can put human life at risk, and hence security inside BANs is a critical issue. Safe distribution and periodic refreshment of cryptographic keys are needed to ensure the highest level of security. In this paper, we focus on the key distribution techniques and how they are categorized for BAN. The state-of-art pre-shared key distribution algorithms are surveyed. Possible attacks on algorithms are demonstrated with examples.

Keywords : attacks, body area network, key distribution, key refreshment, pre-shared keys
Conference Title : ICBAN 2016 : International Conference on Body Area Networks
Conference Location : New York, United States
Conference Dates : October 10-11, 2016